7 World Wide Web (WWW)

The Internet, as described in the Introductory section of this document, is a network of networks, providing the infrastructure for communication and sharing of information. It provides a number of services including e-mail, file transfer, login from remote systems, interactive conferences, news groups, and the World Wide Web.

The World Wide Web (known as "WWW', "Web" or "W3") is the universe of Internet-accessible information. The World Wide Web began as a networked information project at CERN, the European Laboratory for Particle Physics. The Web has a body of software, and a set of protocols and conventions used to traverse and find information over the Internet. Through the use hypertext and multimedia techniques, the web is easy for anyone to roam, browse, and contribute to.

Web clients, also known as web browsers, provide a user interface to navigate through information by pointing and clicking. Web servers deliver HTML (Hyper Text Markup Language) and other media to browsers through the Hyper Text Transfer Protocol (HTTP). The browsers interpret, format, and present the documents to users. The end result is a multimedia view of the Internet.

Web servers can be attacked directly, or used as jumping off points to attack an organization's internal networks. There are many areas of Web servers to secure: the underlying operating system, the Web server software, server scripts and other software, etc.

Browsers also introduce vulnerabilities to an organization, although generally less severe than the threat posed by servers. The following sections provide policy samples for the use of World Wide Web browsers, servers, and for publishing information on World Wide Web home pages.

7.1 Browsing the Internet

There are a number of risks related to the use of WWW browsers to search for and retrieve information over the Internet. WEB browsing programs are very complicated and getting more complicated all the time. The more complicated a program is, the less secure it generally is. Flaws may then be exploited by network-based attacks.

7.2 Example Browsing Policies

Low Risk

User

Software for browsing the Internet such as WWW, Gopher, WAIS, etc. is provided to employees primarily for business use.

Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass the company.

Company Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing.

Users of the WWW are reminded that Web browsers leave "footprints" providing a trail of all site visits.

Manager

Approved sources for licensed WWW software will be made available to users.

Technical

A local repository of useful WWW browsers, helper applications and plug-ins will be maintained and made available for internal use.

Medium Risk

User

Software for browsing the World Wide Web is provided to employees for business use only.

All software used to access the WWW must be approved by the Network Manager and must incorporate all vendor provided security patches.

Any files downloaded over the WWW shall be scanned for viruses, using approved virus detection software.

Due to the non-secure state of the technology, all WWW browsers shall disable the use of Java, JavaScript, and ActiveX

Only company approved versions of browser software may be used or downloaded. Non-approved versions may contain viruses or other bugs.

All WEB browsers shall be configured to use the firewall http proxy.

When using a form, ensure that the SSL or Secure Sockets layer or other such mechanism is configured to encrypt the message as it is sent from the user's browser to the Web server.

Manager

Technical

High Risk

User

Users may browse the Internet using World Wide Web (WWW), Gopher, WAIS, etc., for the sole purpose of their research or job function.

No sites known to contain offensive material may be visited.

Any user suspected of misuse may have all transactions and material logged for further action.

URLs of offensive sites must be forwarded to the COMPANY Web security contact.

Manager

A company-wide list of forbidden sites will be maintained. WWW software will be configured so that those sites cannot

Internet sites containing offensive material will be immediately blocked by network administrators.

Contractors must follow this policy after explicit written authorization is given for access to the Internet.

Technical

All sites visited are logged.

Web browsers shall be configured with the following rules:

They will only access the Internet through the firewall HTTP proxy.

They will scan every file downloaded for viruses or other malign content.

Only ActiveX controls signed by the COMPANY may be downloaded.

Only Java signed by the COMPANY may be downloaded.

Only JavaScript signed by the COMPANY may be downloaded.

Web pages often include forms. As with e-mail, data sent from a Web browser to a Web server passes through many interconnecting computers and networks before reaching its final destination. Any personal or valuable information sent using a Web page entry may be eavesdropped on.

7.3 Web Servers

Many organizations now support an external WWW Web site describing their company or service. For security reasons servers are usually posted outside the company firewall. Web sites range from home-spun notices, to carefully developed and designed marketing vehicles. Organizations may spend a considerable amount of money and effort into developing a Web site that is informational yet non-cumbersome, or that creates the right company logo or style. In a sense, an organization's Web site forms a piece of the company's image and reputation.

The creation, management, and maintenance of a company's external Web site should be assigned. In larger companies, Internet Web site responsibilities may be spread across several position groupings. For example, a Director of online business development may be responsible for identifying and implementing new business opportunities while the Web site manager oversees the overall strategy of the Web site including coordinating content preparation, distribution, and budget monitoring. A Director of on-line sales/marketing may be responsible for advertising revenue generation related to the Web site. A Web site engineer or Webmaster would responsible for the technical aspects of the Web site, including development, connection, Intranet, e-mail, and firewall security. There would most likely be programmers for the operational aspects of the Web site, including installations, design, coding, debugging, and documentation of the Web site. A Web site artist may create the graphic and content aspects.

In a smaller organization, a Web site engineer or Webmaster may assume most of the above responsibilities and report to a marketing or Public Relations manager. In the smallest of companies, a system analyst or system/LAN administrator may be given the additional role. Whatever manner the Web site is administered, this role or series of roles enforces company policy that is defined by management. Senior management, such as the Director of online business development in the above large company example, should be the designated authority to approve new or revised external Web sites prior to posting.

Additionally, internal company Web sites which are inside the company firewall are often used for posting company information to employees. Information such as birthdays, corporate calendars, phone directories, etc., are often posted. Internal Web sites are also used for internal project information, providing a central point of reference for the project team. Although internal Web sites do not carry the same visibility as external pages, they do need to be managed with system specific guidance and procedures. The project leader generally takes on this responsibility.

Anyone can create a Web site for posting information that is non-company related. A company must determine whether they will allow personal home pages through the company's Internet service, or whether employees may only do so through their own Internet service provider.

As described in section 7.3 on Web sites, most organizations deploying an Internet do so to offer information or services to the public. Because they are presenting information, rather than hiding it, they often describe the web site a "public" web site; nothing confidential is on the web server, so there is no danger or threat there. The problem with this attitude is that while the information

may be publicly available, the web site is an extension of the organizations that owns it and must be secure form vandalism.

Public web sites of MGM/Universal Studios, the Nation of Islam, The U.S. Department of Justice, and the U.S. Central Intelligence Agency can identify with this statement. They all had break-ins to their public sites in 1996. The attackers exploited weaknesses in the base operating systems on which the web servers ran. They broke into these sites with apparent ease, modified information, in some instances added pornographic photos, and in one case inserted hateful language.

While public embarrassment may be the only consequence in these cases, this may be significant enough not to want to bear the consequence a second time! Had the attackers modified a company's statements of services, falsified prices, etc., consequences could be more severe.

7.4 Example Web Server Policies

Low Risk

User

No offensive or harassing material may be made available via COMPANY Web sites.

No personal commercial advertising may be made available via COMPANY Web sites.

Manager

Managers and users are permitted to have a Web site.

The personal material on or accessible from the Web site is to be minimal.

No offensive or harassing material may be made available via COMPANY Web sites.

No Company confidential material will be made available.

Technical

A local archive of Web server software and authoring tools will be maintained and made available for internal use.

Medium Risk

User

Users are not permitted to install or run Web servers.

Web pages must follow existing approval procedures regarding company documents, reports, memos, marketing information, etc.

Manager

Managers/Users are permitted to have Web pages for a business-related project or function.

Technical

The Web server and any data to be accessed by the general public must be located external to the company firewall.

Web servers shall be configured so users cannot install CGI scripts.

All network applications other than HTTP should be disabled (e.g., SMTP, ftp, etc.)

Information servers shall be located on a screened subnet to isolate itself from other site systems. This reduces the chance that an information server could be compromised and then used to attack site systems.

If using a Web administrative tool, restrict access to only authorized systems (via IP address, rather than hostname). Always change default passwords.

High Risk

User

Users are forbidden to download, install or run Web server software.

Network traffic will be monitored for unapproved Web servers, and operators of those servers will be subject to disciplinary action.

Manager

The CIO must approve the operation of any other web server to be connected to the Internet in writing.

All content on company WWW servers connected to the Internet must be approved by and installed by the Web Master.

No confidential material may be made available on the Web site

Information placed on the Web site is subject to the same Privacy Act restrictions as when releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information. Copyrights must be protected and permission obtained before placing copyrighted information on the Web site Contact public affairs or legal authorities for advice and assistance.

All publicly accessible Web sites must be thoroughly tested to ensure all links work as designed and are not "under construction" when the site is opened to the public. Under construction areas are not to appear on publicly accessible Web sites.

Technical

There shall be no remote control of the Web server (i.e., from other than the console.) All administrator operations (e.g., security changes) shall be done from the console. Supervisor-level logon shall not be done at any device other than the console.

The Web server software, and the software of the underlying operating system, shall contain all manufacturer recommended patches for the version in use.

Incoming HTTP traffic will be scanned, and connections to unapproved Web sites will be reported.

Restricting user access to addresses ending in .GOV or .COM provides a minimal level of protection for information not cleared for release to the public. A separate server or partition may be used to separate restricted use information (internal company information or internal Web site) from information released to the public.

All Web sites may be monitored as part of the company's network administration function. Any user suspected of misuse may have all their transactions logged for possible disciplinary action.

On UNIX systems, Web servers shall not be run as root.

The implementation and use of CGI scripts shall be monitored and controlled. CGI scripts shall not accept unchecked input. Any programs that run externally with arguments should

not contain metacharacters. The developer is responsible for devising the proper regular expression to scan for shell metacharacters and shall strip out special characters before passing external input to the server software or the underlying operating system.

All company WWW servers connected to the Internet will have a firewall between the Web server and internal company networks. Any internal WWW servers supporting critical company applications must be protected by internal firewalls. Sensitive, confidential, and private information should never be stored on an external WWW server.